Citizen Lab Testimony on NSO Group: One-sided, Short-sighted, and Misleading

On July 27, 2022, the House Permanent Select Committee on Intelligence (HPSCI) conducted a hearing predominantly based on testimony by the Citizen Lab, a Canadian organization that has issued a series of misleading, inaccurate, incomplete, and one-sided reports on NSO Group for nearly a decade.

Citizen Lab reports are not independently validated beyond a "peer review" by Amnesty International, a well-known anti-Israel organization and advocate for the Boycott, Divestment, Sanctions (BDS) movement. Additionally, Citizen Lab reports are often unable to differentiate between NSO's tools and those of other cyber intelligence companies in operation. Review by NSO Group is the only way to truly verify the accuracy of Citizen Lab's data, but Citizen Lab is, instead, motivated to report predetermined outcomes which intentionally mislead the public. Further, any discussion on cyber intelligence tools must include the threats and challenges law enforcement across the world face from the growing misuse of end-to-end encryption applications by terrorists and criminals who use them to conceal messages and plots when communicating through mobile devices. No members of law enforcement or of the intelligence community testified at the HPSCI hearing. NSO welcomes public debate on the use of cyber intelligence capabilities, including the need for a global regulatory framework to help governments and the private sector ensure the proper use of these lifesaving tools.

✖ MYTH: 50,000 phone numbers were targeted by Pegasus.

✓FACT: Pegasus has not been deployed against anywhere close to 50,000 numbers.

In July 2021, Citizen Lab, as part of the Pegasus Project, reported a list of 50,000 phone numbers that supposedly represented potential targets of NSO's Pegasus technology. The Washington Post, part of the Pegasus Project, acknowledged that "[t]he list does not identify who put the numbers on it, or why, and it is unknown how many of the phones were targeted or surveilled."

The 50,000 number of purported targets is entirely implausible based on the number of licenses actually granted by NSO. The list of "targets"— for which no details or source have been publicly disclosed — is not a list of Pegasus targets nor has it been taken from the Pegasus system. Furthermore, there is no consolidated list of targets or potential targets, nor a server which holds such information. Prominent numbers from the list have been verified by NSO as never having been targets of Pegasus by any NSO customers.

Further, NSO 1) does NOT control or know which individuals are targeted by Pegasus, 2) does NOT participate in any of their customers' intelligence operations, and 3) as dictated by NSO's Human Rights Policy, terminates customer access to Pegasus when it learns of actual or potential misuse.

NSO 1) provides a very limited number of licenses to its government customers, 2) utilizes stringent commercial contracts with its customers that allow the company to conduct a fast and thorough inquiry into misuse of the technology and 3) itself and its customers are strictly regulated by the Israeli Ministry of Defense.

✖ MYTH: Pegasus targets Americans.

✓FACT: Pegasus is configured to prevent targeting of any +1 mobile numbers, or phones on US soil, unless an exception is made for a U.S. government entity.

Citizen Lab testified that it identified "many" U.S. citizens and U.S. public officials targeted by Pegasus, but then conveniently refused to name them. U.S. government officials could only have been targeted while using non-+1

Received by NSD/FARA Registration Unit 09/08/2022 3:13:44 PM

numbers. Immediately after being alerted to an allegation that U.S. officials using Ugandan phone numbers were potentially targeted, NSO immediately terminated all possible relevant contracts — despite there being no indication or proof that the phones were, in fact, targeted by Pegasus — based entirely on the seriousness of the allegations.

✖ MYTH: Pegasus Represents a Uniquely Dangerous Counter-Intelligence Threat

✓FACT: A myriad of controls prevent Pegasus from representing a counter-intelligence threat to U.S. interests, and NSO Group is open to additional controls suggested by the U.S. Government.

In addition to not monitoring +1 numbers, software controls set the Pegasus system to "self-destruct" if there is an attempt to transfer or copy it, and NSO has the ability to remotely terminate the system at any time for any reason, including for violations of NSO's Human Rights Policy or Israeli MOD export controls. In fact, NSO has terminated contracts with multiple customers, after misuse of its technology was discovered.

NSO has a robust Human Rights Policy – the first of its kind in the industry – that includes extensive due diligence prior to a sale and ongoing monitoring after a sale is made. NSO has cooperated repeatedly with governmental investigations to determine misuse and promptly publicized any findings. **In fact, NSO has turned down over $300 million in business** from such investigations and/or countries that pose an unacceptably high risk of product misuse.

As noted in the hearing, "**we are not putting this genie back in the bottle."** NSO Group has and continues to call for the establishment of an appropriate international legal framework, sector-specific standards for states and companies, and guidelines to better determine criteria for legitimate end users of these crucial intelligence systems.

Further, public reporting has noted that **the U.S. intelligence community has funded the purchase of Pegasus by foreign governments.**

✖ MYTH: A "zero-click" exploit is entirely new technology.

✓FACT: By Citizen Lab's definition, the traditional wiretap is a "zero-click" exploit.

Citizen Lab testimony described a "zero-click" exploit as meaning "that the victim doesn't have to click or open a file or perform any other action in order to be infected." What Citizen Lab fails to note is that such a definition would also apply to the traditional wiretap, used by law enforcement in democracies across the globe. **Further, just like a traditional wiretap, Pegasus is used with specific, pre-identified phone numbers, one at a time, and is** the only such type of target centric solution.

✖ MYTH: Pegasus and cyber intelligence tools are not used to prevent crime and terrorism.

✓FACT: Pegasus has helped save thousands of lives, but NSO is prohibited from publicly reporting successes.

Citizen Lab testimony provided **an extremely limited and misleading view of the overall use of cyber intelligence tools and no insight into the lives that NSO technology has helped save.**

Under Israeli law, NSO is prohibited from disclosing its successes, which are vastly larger than the claimed examples of misuse. NSO can note, however, that Pegasus technology has been repeatedly used to thwart suicide bombings, breakup terrorist rings, and even capture fugitive drug lords accused of multiple murders — including of journalists — and wide-

Received by NSD/FARA Registration Unit 09/08/2022 3:13:44 PM

scale drug trafficking. Belgium's privacy minister even noted that tools like Pegasus are more effective and safer at investigating crimes than software "backdoors."

Through the use of Pegasus, state authorities have and continue to thwart numerous terrorist attacks such as suicide bombings, and has been instrumental in apprehending pedophiles and other serious criminals.

NSO is fully aware of and committed to its own human rights responsibilities and those of its customers, and is determined that its products be used appropriately and lawfully. NSO takes concrete steps to ensure these critical technologies are used for the purpose they were designed for – saving lives without compromising the public's privacy.

Received by NSD/FARA Registration Unit 09/08/2022 3:13:44 PM